UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/918,188	07/30/2001	Keith Alexander Harrison	30003040-2	2580

7590 02/10/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SCHUBERT, KEVIN R	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/10/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/918,188	HARRISON ET AL.	
	Examiner	Art Unit	
	Kevin Schubert	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *07302001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-63 have been considered.

Title

A new title is suggested by the examiner. The current title "Document Transmission Techniques I" is not descriptive. The examiner suggests "Authentication Method in a Printing Environment". A new title is suggested but not required.

Claim Objections

Claim 21 is objected to because of the following informalities: the examiner believes "transmitting" as referred to in part c) should be "receiving". The system is disclosed so that the printout station receives a document and securely retains it. The examiner assumes the applicant meant "receiving and securely retaining" the document. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-2,5-6,8-11,13-18,41-43,46-48,54-56,58, and 60-62 are rejected under 35 U.S.C. 102(b) as being anticipated by Mandelbaum, European Patent Application Publication No. 0671830 A2.

As per claim 1, the applicant describes a method of delivering a digital document to an intended recipient at a printout station comprising the following limitations which are met by Mandelbaum:

a) receiving and securely retaining a transmitted document and a transmitted independently verifiable data record of the intended recipient at a printout station (Col 6, lines 40-44; Col 2, lines 9-26);

b) obtaining a first token of the intended recipient (Col 2, lines 50-53);

c) requesting proof of the intended recipient's identity at the printout station using data in the independently verifiable data record of the intended recipient (Col 6, lines 56-58; Col 7, lines 1-6; Col 5, lines 49-58; Table 10 of Fig 4);

d) releasing the document when the intended recipient has proven their identity by use of a second token that is uniquely related to the first token (Col 7, lines 27-47);

Regarding part a), messages sent to the printout station comprise an unrestricted access part which identifies the intended recipient and is the independently verifiable data record (Col 2, lines 9-26) and a restricted access part which is securely stored in memory until the intended recipient has proven his identity (Col 2, lines 9-26; Col 6, lines 40-44).

Regarding parts b) and d), the applicant writes that the first token is a public key when public-key infrastructure is being used (Applicant: Page 4, lines 15-16). Mandelbaum writes that the sender uses a public key, or first token, of the recipient in order to encrypt a message which can only be decrypted by the use of the recipient's private key, or second token, which is uniquely related to the second token (Col 7, lines 27-47). The recipient therefore obtains the first token since the message is encrypted using the first token. The applicant should also note that in a second embodiment which is less secure, the sender can use his private key to encrypt a message which can only be decrypted using the sender's public key.

Regarding part c), the lines and figure referenced above illustrate that the intended recipient must prove his identity to the fax machine (which uses the stored independently verifiable data record obtained in the header portion of the message) in order to decrypt and access the restricted message portion.

As per claims 2 and 42, the applicant describes the method of claims 1 and 41, which are anticipated by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the transmitted document is a fax document and the printout station comprises a fax machine (Col 3, lines 15-17).

As per claims 5 and 46, the applicant describes the method of claims 1 and 41, which are anticipated by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the retaining step comprises storing the received document in memory without printing out a copy of it on receipt (Col 6, lines 40-44).

As per claims 6 and 47, the applicant describes the method of claims 5 and 46, which are anticipated by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step comprises printing out a copy of it (Col 7, lines 48-56);

As per claim 8, the applicant describes the method of claim 1, which is anticipated by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step is carried out when the intended recipient has presented a portable data carrier holding the second token to the printout station and has transferred data to prove their identity (Col 7, lines 27-56);

The portable data carrier, or smart card, must be presented to the smart card interface to prove their identity. Also, the smart card holds the intended recipient's private key, or second token, which is used to decrypt the encrypted message.

As per claims 9 and 48, the applicant describes the method of claims 8 and 41, which are met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step further comprises the intended recipient entering a verifiable security identifier into the printout station to establish that they are the legitimate owner of the portable data carrier (Col 4, lines 21-24);

The identifier is the PIN code.

As per claim 10, the applicant describes the method of claim 8, which is met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the portable data carrier is a smart card and the printout station comprises a smart card reader (Col 4, lines 9-13).

As per claim 11, the applicant describes the method of claim 1, which is met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the obtaining step comprises extracting the first token transmitted with the document and the data record (Table 404 of Fig 4);

As one can see in the table, the fax machine is able to extract information about the first token from the message and display the information as a flag which is set when the message is encrypted with the intended recipient's public key.

As per claim 13, the applicant describes the method of claim 1, which is met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Further comprising carrying out an on-line check of the validity of the intended recipient's independently verifiable data record (Col 4, lines 17-24);

The applicant writes that the smart card authentication method is preferably the AT&T CSS user authentication system "in which the user calls the system" (Col 4, lines 17-19). Since the user is calling the system for authentication, an online authentication is taking place.

As per claim 14, the applicant describes the method of claim 1, which is met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Further comprising instructing a third party to carry out an on-line check of the validity of the intended recipient's independently verifiable data record (Col 4, lines 17-24);

Since the authentication system is one in which the user calls into the system, it is reasonable to assume that a third party validates the intended recipient.

As per claims 15 and 16, the applicant describes the method of claims 13 and 14, which are met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the releasing step further comprises only releasing the document if the validity of the independently verifiable data record has been confirmed as a result of the check (Col 4, lines 23-24).

As per claims 17 and 43, the applicant describes the method of claims 1 and 41, which are met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the first and second tokens comprise private and public encryption/decryption keys of the intended recipient (Col 2, lines 50-53; Col 7, lines 27-32);

The use of the recipient's public key, or first token, is described (Col 2, lines 50-53) as well as the use of the intended recipient's private key, or second token, (Col 7, lines 27-32).

As per claim 18, the applicant describes the method of claim 1, which is met by Mandelbaum (see above), with the following limitation which is also anticipated by Mandelbaum:

Wherein the transmitted document is encoded and the method further comprises decoding the received document once the intended recipient has proven their identity (Col 7, lines 3-6; Col 7, lines 27-56).

As per claim 41, the applicant describes a device for delivering a digital document to an intended recipient comprising limitations a) through d) which are met by Mandelbaum in the rejection of claim 1 (see above) and the following additional limitation which is also met by Mandelbaum:

e) a portable data carrier reader for receiving information from a portable data carrier (Col 4, lines 9-13).

As per claim 54, the applicant describes a method of delivering a digital document from a first station via a communications network to an intended recipient at a second station, the method comprising limitations d) through g) which are met by Mandelbaum in the rejection of claim 1 (see above) and the following additional limitations which are also met by Mandelbaum:

a) obtaining details of the intended recipient, including an independently verifiable data record of the intended recipient at the first station (Col 5, lines 5-11);

b) determining prior to transmission of the document whether the second station is one which is arranged to implement the present method (Col 5, lines 5-11);

c) transmitting the document and the independently verifiable data record of the intended recipient to the second station (Col 5, lines 29-33);

Regarding part b), the applicant should note that it is inherent in the art that the address book provides a way of determining whether the second station is one which is arranged to implement the present method. Otherwise, it wouldn't make sense to keep an address book of intended recipients and the public keys if the intended recipients had no way to decrypt the received message according to the present system.

As per claims 55 and 61, the applicant describes the method according to claims 54 and 60, which are met by Mandelbaum (see above), with the following limitation which is also met by Mandelbaum:

Further comprising obtaining details of the intended recipient including the independently verifiable data record prior to transmitting the document (Col 5, lines 5-27).

As per claims 56 and 62, the applicant describes the method according to claims 55 and 61, which is met by Mandelbaum (see above), with the following limitation which is also met by Mandelbaum:

Wherein the step of obtaining details comprises obtaining the independently verifiable data record from a central database storing many possible intended recipients' details (Col 5, lines 9-11).

As per claim 58, the applicant describes the method of claim 54, which is met by Mandelbaum (see above), with the following limitation which is also met by Mandelbaum:

Further comprising encoding the document prior to transmitting it to the second station and decoding the received document once the intended recipient has proven their identity (Col 5, lines 33-40; Col 7, lines 27-44);

The use of encoding or encrypting the document is described (Col 5, lines 33-40) as is the use of decoding or decrypting the document (Col 7, lines 27-44).

As per claim 60, the applicant describes a method of delivering a digital document from a first station via a communications network to an intended recipient at a second station comprising limitations b) through f) which are met by Mandelbaum in claim 54 (see above) and the following additional limitation which is also met by Mandelbaum:

a) obtaining details of the intended recipient, including an independently verifiable data record of the intended recipient at the first station, encoding the document using encryption techniques prior to transmitting it to the second station (Col 5, lines 5-10; Col 5, lines 33-40).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3-4,44-45, and 49-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Lundblad, European Patent Application Publication No. 0542703 A1.

As per claims 3-4 and 44-45, the applicant describes the method of claims 1 and 41, which are met by Mandelbaum (see above), with the following additional limitation which is met by Lundblad:

Wherein the retaining step comprises printing out the document as received and placing it in a locked compartment (Col 3, lines 3-12; 14 of Fig 1);

Mandelbaum discloses all the limitations of the independent claims 1 and 41. However Mandelbaum fails to disclose the use of a locked compartment for storing the documents.

Lundblad discloses a fax transmission apparatus which includes the use of a locked compartment where documents can be stored until opened by the intended recipient who proves his identity by using a physical key to unlock the compartment. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Lundblad with those of Mandelbaum because the incorporation of the two systems provides another way to securely retain documents until an authorized person has access to receive them.

Regarding claims 4 and 45, only an authorized person who has the proper key can release the documents from the locked compartment.

As per claim 49, the applicant describes a device for delivering a digital document to an intended recipient, the device comprising limitations a) through d) which are met by Mandelbaum (see the rejection for claim 1) with limitation e) which is met by Lundblad (see the rejection for claim 3).

As per claims 50-53, the applicant repeats claims that have already been rejected by Mandelbaum but are now rejected under U.S.C. 103(a) in light of Mandelbaum in view of Lundblad

because they depend on independent claim 49 which is rejected by Mandelbaum in view of Lundblad. The applicant should note that claim 50 corresponds to claim 4, claim 51 corresponds to claim 2, claim 52 corresponds to 17, and claim 53 corresponds to claim 9.

Claims 7,12,57, and 63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum.

As per claim 7, the applicant describes the method of claim 1, which is met by Mandelbaum (see above), with the following limitation which is also met by Mandelbaum:

Wherein the requesting step comprises requesting supply of data encoded with the second token which can be decoded with the first token (Col 6, lines 56-58; Col 7, lines 1-6);

Mandelbaum discloses that an intended recipient's second token, or private key, is stored on a smart card which is authenticated at the fax machine. Mandelbaum also discloses that the fax machine has a way of extracting information in the header which discloses that the sender is using the recipient's public key (Table 404 of Fig 4).

However, Mandelbaum never discloses that the authentication of the smart card is done via requesting data encoded with the second token which can be decoded and verified by the first token. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate this authentication method because this is an authentication method which could be easily implemented in the system.

As per claims 12,57, and 63, the applicant describes the method of claims 11,54, and 60, which are met by Mandelbaum (see above), with the following additional limitation which is also met by Mandelbaum:

Wherein the intended recipient's independently verifiable data record is provided as an intended recipient's digital certificate (Col 2, lines 38-40);

Mandelbaum discloses all the limitations of claim 11. While Mandelbaum discloses the need for authenticating the intended recipient, he does not disclose the use of a digital certificate sent from the sending fax machine. One method Mandelbaum proposes is having the user insert his smart card into the fax apparatus to authenticate the user's identity.

It would be obvious to authenticate the user's identity through a certificate in light of Mandelbaum's system. In such a system, data on the smart card could be checked with data on the certificate to authenticate the user's identity.

Claims 19-37, and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Auerbach, European Patent Application Publication No. 0798892 A2.

As per claims 19 and 59, the applicant describes the method of claims 18 and 58, which are anticipated by Mandelbaum (see above), with the following limitation which is anticipated by Auerbach:

Wherein the transmitted document has been encoded using enveloping technique and the decoding step comprises using enveloping decryption techniques (Col 3, lines 5-10; Col 3, lines 26-30);

Mandelbaum describes all the limitations of claim 18. However, Mandelbaum fails to disclose the use of enveloping encryption and decryption techniques.

Auerbach discloses a method for the creation and distribution of digital documents using the methods and techniques of secure cryptographic envelopes (Col 1, lines 3-8). Cryptographic envelopes provide an extra layer of security for messages because they comprise superencrypting a message. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Auerbach with those of Mandelbaum so that the transmitted message is encoded using enveloping technique for extra security.

As per claim 20, the applicant describes the method of claim 19, which is anticipated by Mandelbaum in view of Auerbach (see above), with the following limitations which are anticipated by Auerbach:

a) the transmitted document has been encoded with a session key and the session key has been encrypted with the first token (Col 2, lines 56-58; Col 3, lines 1-10);

b) the transmitting step comprises transmitting the encrypted session key to the printout station (Col 2, lines 56-58; Col 3, lines 1-10);

c) the decoding step comprises decrypting the encrypted session key with the second token and decoding the received document with the decrypted session key (Col 3, lines 26-30);

Regarding part a), the transmitted document is encoded with a session key which corresponds to the part encryption key disclosed by Auerbach. Auerbach further discloses that the part encryption key, or session key, is encrypted using a first public key, which would correspond to the intended recipient's public key if the ideas of Auerbach were combined with the ideas of Mandelbaum.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Auerbach with those of Mandelbaum in light of the fact that superencryption via a session key and a public key provides an additional layer of security.

As per claim 21, the applicant describes a method of delivering a digital document to an intended recipient at a printout station comprising limitations a) and c) through e) which are met by Mandelbaum (see rejection for claim 1) and limitations b) and e) which are met by Auerbach (see rejection for claim 20).

As per claims 22 and 25-37, the applicant repeats claims 2 and 5-17 which have already been rejected by Mandelbaum (see above). Claims 22 and 25-37 are rejected under U.S.C. 103(a) because they are dependent on the system of claim 21 which is met by Mandelbaum in view of Auerbach (see above).

Claims 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Auerbach in further view of Lundblad.

Claims 23 and 24 are repeats of claims 3 and 4 which are rejected by Mandelbaum in view of Lundblad (see above). Claims 23 and 24 must be rejected under Mandelbaum in view of Auerbach in further view of Lundblad because the claims depend on claim 21 which is met by Mandelbaum in view of Auerbach.

Claims 38 and 39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Auerbach in further view of Schneier (Schneier, Bruce. Applied Cryptography. 1996. John Wiley & Sons, Inc. Second Edition. Pages 68-73).

As per claim 38, the applicant describes the method of claim 21, which is anticipated by Mandelbaum in view of Auerbach (see above), with the additional limitation that the system involves a plurality of users and not just one user which is met by Schneier (pages 68-73).

Mandelbaum in view of Auerbach describe all the limitations of claim 21. However Mandelbaum in view of Auerbach fails to disclose the use of a plurality of users. Schneier discloses a secret splitting method whereby more than one intended recipient is needed to be present to allow a process to happen (page 70-71).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Mandelbaum in view of Auerbach in the case where more than one recipient needs to prove his identity at the printing station for a document to be printed.

As per claim 39, the applicant describes the method of claim 38, which is anticipated by Mandelbaum in view of Auerbach in further view of Schneier, with the following additional limitation which is also met by Schneier:

Wherein the transmitted document or a session encryption/decryption key of the transmitted document has been sequentially encrypted with each of the first tokens of the intended recipients in a given order and the processing step comprises sequentially decrypting the transmitted document or a

session encryption/decryption key with each of the second tokens of the intended recipients in the reverse of the given sequential order (page 68-69).

Mandelbaum in view of Auerbach in further view of Schneier describe all the limitations of claim 38. Schneier also discloses the use of multiple key cryptography where a message can be encrypted with more than one public key so that the intended recipients need to present their private keys in a particular order to decrypt a message.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Schneier with those of Mandelbaum in view of Auerbach in the case where more than one recipient needs to prove his identity at the printing station for a document to be printed.

Claims 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mandelbaum in view of Schneier.

As per claim 40, the applicant describes a method of delivering a digital document which is met by Mandelbaum (see the rejection for claim 1) with the additional limitation of incorporating the use of a plurality of intended recipients which is met by Schneier (see the rejection for claim 38).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER